New technological developments in the blockchain space.

zkSNARKs for scaling and privacy.

Alexandre Poltorak

Workshops on Blockchain and GDPR
8. April 2019 – Geneva, Switzerland

Bitcoin & Privacy

A blockchain is a public, shared database that records transactions between two parties. Specifically, blockchains document and confirm who owns what at a particular time through cryptography. After a particular transaction is validated and cryptographically verified by other participants, or nodes in the network, it is then made into a "block" on the blockchain. A block contains information about when the transaction occurred, previous transactions, and details about the transaction. Once recorded as a block, transactions are ordered chronologically and cannot be altered or changed.

- from Wikipedia https://en.wikipedia.org/wiki/Privacy_and_blockchain

- https://bitcoin.org/en/protect-your-privacy

zkSNARKs for scaling and privacy.

ZkSNARKs - Zero-Knowledge Succinct Non-Interactive Argument of Knowledge

ZKPs allow for greater privacy on public blockchains by enabling nodes, or network participants, to verify the existence and validity of transactions, and therefore maintain distributed consensus, without actually being able to see or make public any of the transaction details, guaranteeing privacy.

“With zero-knowledge proofs, organizations can transact on the same network as their competition in complete privacy and without giving up the security of the public Ethereum blockchain." - EY

zkSNARKs provides the ability to verify the correctness of computations without having to execute them.

https://z.cash/ is a privacy-protecting, digital currency. It was the first to widely spread ZKP and zkSNARKs technology.

Coda Protocol

Coda is a scalability solutions using recursive zkSNARKs or recursive proof-composition. Coda swaps the traditional blockchain for a tiny cryptographic proof, enabling a cryptocurrency as accessible as any other app or website.

20 kB

Other solutions based on zkSNARKs

- Off-chain scaling using zkSNARKs (sidechains)
- Iden3 – claims-based identity management
- zk-DAI
- Circom

https://zeroknowledge.fm